PX 452

Message

From: Brad Garlinghouse [redacted]@gmail.com]
Sent: 7/9/2015 4:56:42 PM
To: Patrick Griffin [Patrick Griffin [redacted]
CC: Monica Long [Monica Long <[redacted]
Subject: Fwd: FW: Blockchains / Ripple
Attachments: ripple_deep_dive_for_financial_professionals.pdf

Patrick - see below. This is the guy I referenced earlier today.

Can you send me white paper's that I can forward? In particular he wants to see our "counterpoint" to the bitcoin community criticisms

Also, assuming you are comfortable, will you do an intro for him and Phil?

Monica - fyi. But please send aggregated new stuff that I can forward on to [redacted]

---------- Forwarded message ----------
From: [redacted]
Date: Thu, Jul 9, 2015 at 3:23 PM
Subject: FW: Blockchains / Ripple
To: [redacted]
Cc: [redacted]

Brad, Thanks so much for your time today – I enjoyed meeting you and talking about the growth in the business. Love a place with customers lined up outside – now we need to monetize them and their customers! Please send whitepapers, as I want to learn as much as I can so I can think strategically about the opportunity. Any further thoughts your team has on [redacted] integration with [redacted] and how that affects you also is helpful. Again it appears a retail driven strategy but again, volume is volume and website integration is massive. Obviously Amazon must be watching quite closely.

I hope to follow up with more thoughts and questions as the days progress. Can you also put me in touch with your marketmaker who is based in NY? I'd love to talk to him about his strategy and what he is seeing.

Gratefully,

(Notes referenced on XRP/Block ledgering appended below, as discussed)

Here is a first draft summary of my thoughts on XRP/Ripple. I think it has value, it is more than a check – it is a credit-less 'check' with immediate payment and only so many are available (ie, limited supply). Effectively it is fungible gold. But they have no lock on ledger systems, they will win by driving adoption and being incorruptible (i.e. why gold better than other more common stores of value). I like their approach of being a system friendly clearing agent, but I have trouble predicting their success versus others (competition and adoption difficult to predict). Processing speed gives them an enormous advantage over Bitcoin.

Summary:

1) Ripple should prove a store of value like gold and Bitcoin (it is not a check, since total amount of Bitcoin (BTC) and Ripple coins (XRP) 'checks' in issue is known and limited). XRP's relative advantages are that it is **more efficient to transfer** (faster than bitcoin/gold) and **more network friendly** (more established counterparties can use it and the open protocol).

2) Areas of concern are a) market adoption drivers (**what drives market share?**) b) natural **transaction limits** of consensus recognition/verification mechanism (1,000 per second vs Visa 10,000 per second) and c) **'treasury' stock** held by Ripple Labs and future issuance/distribution mechanisms (**dilution**).

What is it worth?

XRP currently trade for 0.01c per XRP, giving it a 'market cap' of $1bil (100bil 'coins' in issue). Bitcoin (BTC) market cap is $4bil for the 14.3m 'mined' coins (about 70% of 21m total have already been 'mined'). Total gold in issue trades for approximately $6tril. Could a crypto-currency trade for 10% of gold, or $600bil? That is 150fold gain (+1500%) for Bitcoin **if worth 10% of gold in issue**. That is 600fold gain (+6000%) for XRP.

First-Adopter / Network Effects / Best Block Ledger

There is likely an Esperanto / USD reserve currency effect to being first and most widely used. How sticky these effects are debatable. Further, whether a better block ledger is distributed is of course a question. But if enough adopt the Ripple Protocol, it may prove to be like SMTP (Simple Mail Transfer Protocol) first defined in 1982 for email movements across the world wide web.

What is Ripple and the Ripple Protocol?

Ripple Labs has developed a block chain transaction protocol that allows any item to be traded and tracked according to a simple ledger system. The ledger system is a common database of encrypted 'owners' which verifies that John bought x from y. This central common ledger avoids an IOU from a central counterparty or a gold coin in your pocket. It is similar to the Bitcoin ledger system.

What is Block Ledgering?

Good description of block ledgering system:

> *Ironically for a technology with such revolutionary potential, the Bitcoin/blockchain operating principle is best explained in terms of ancient forms of exchange. For 500 years or more, stone coins called rai, up to 3.6 metres in diameter, have been used on the Pacific island of Yap. The apparent impracticality of the currency is misleading. Ownership of a coin does not require a physical transfer of the rai stone; the owner passes ownership to a new person by word of mouth, along with the historical record of ownership. Transactions are public, as is ownership. The location of the coin, whether at the top of a mountain or the bottom of the sea, is immaterial. However, reciting the correct record of ownership will soon reveal whether the current owner is in legitimate ownership of the coin.*

What makes Ripple and XRPs interesting:

1) XRP does not need to be mined – thus avoids 'cost' of mining bitcoins

2) Counterparty friendly – it is built to be a settlement system with no credit or counterparty risk and no delays *AND* friendly to existing banking counterparties. It was not designed to disintermediate banks. It is also not a consumer facing interface, it is built instead for financial intermediaries and gateways.

   a. Settlement within 1-5 minutes. Bitcoin takes longer, typically 8-10 minutes.

3) Goal for Ripple: Ripple to Correspondent banking is as email is to the postoffice. Fast, no IOU/Credit cycle, no gatekeeper permissions.

   a. Aim to replace ACH and Swift protocols for money transfers/movements and inter-currency trades.

Value/Market Cap:

1) Gold: about $6trillion (170k tons x $1200/oz x 29167 oz/ton)

2) Bitcoin: about $4bil current (14.3m coins at $275 each). $6mil traded last 24 hrs. (historic high $14bil Dec '13, low $2.5bil Jan '15)

3) XRP: about $1bil current (100,000,000,000 coins at 0.01USD current price), $0.75m traded last 24 hrs, but $2.1m in "payments".

   a. Of note, largest trade types were XRP/JPY and BTC/XRP

Competition:

1) Over 100,000 merchants accept Bitcoin, including PayPal.

Comment from gateway operator:

> *... Working on bitcoin gateway: it is actually easier to move Bitcoin with the ripple protocol since the confirmation process is faster, and you can exchange bitcoin to other types of currencies in the decentralized exchange floor rather than being tied up to 1 centralized exchange floor like Mt. Gox.*

Comment from competitor:

> *Does not think Ripple can do 1k transactions per second. Bitcoin can only do 7 trans per second. Nothing compared with Visa transaction (10k per second).*

Warren Buffett on Bitcoin:

> *"Stay away from it. It's a mirage, basically. ... It's a method of transmitting money. It's a very effective way of transmitting money, and you can do it anonymously and all that. A check is a way of transmitting money, too. Are checks worth a whole lot of money just because they can transmit money? Are money orders? You can transmit money by money orders. People do it. I hope Bitcoin becomes a better way of doing it, but you can replicate it a bunch of different ways, and it will be. The idea that it has some huge intrinsic value is just a joke in my view."*

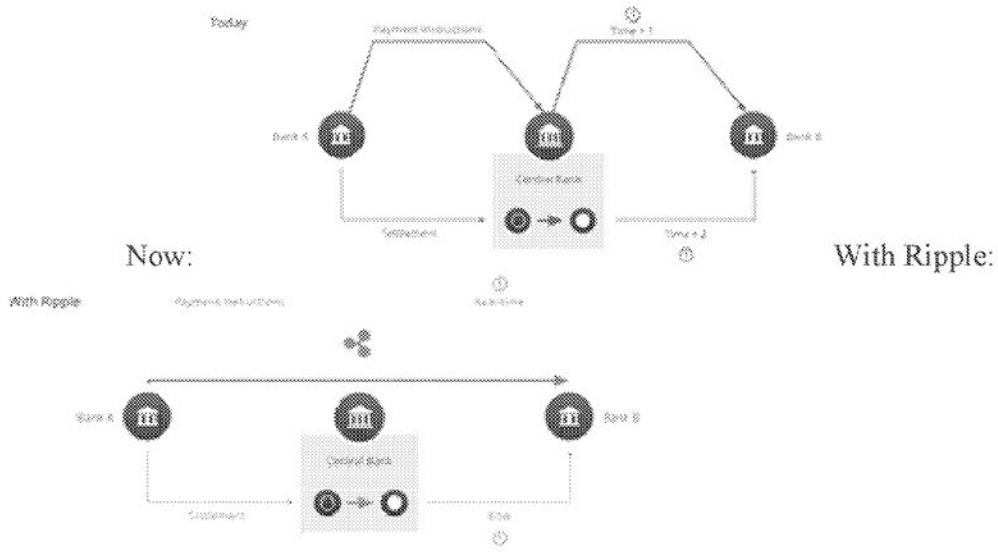
Andreessen Response to Buffett:

> *"A value of a BTC is not arbitrary, in fact it's the opposite of arbitrary," he says. "It equals the value of a single slot in a finite sized public cryptographic ledger through which value can move. The total Bitcoin ledger has value corresponding to the volume and velocity of transactions that will run through it in the future; by extension, each slot in the ledger has fractional value determined by the total number of slots (which, in Bitcoin's case, are limited to 11 million today and 21 million ever)." ... "The market cap of the ledger needs to be high enough to accommodate all of the value that wants to PASS THROUGH it in any period of time (volume & velocity of value passing through)," Andreessen wrote. "So then, the intrinsic value of a BTC is emergent from the functional value of the ledger as a way to exchange value (or, more accurately, emergent from the collective forecast of the future volume & velocity of value that will pass through the ledger)."*

Other:

Many counterparties running pilots on Ripple, including Western Union experimenting with Ripple, here.

Quick visual of settlement cycle vs. correspondent banking:



Now: With Ripple:

Best executive summary:

https://ripple.com/integrate/executive-summary-for-financial-institutions/

Wikipedia has good Bitcoin summary:

https://en.wikipedia.org/wiki/Bitcoin

Three news articles focusing on blockchains:

Good overview:

http://www.economist.com/news/special-report/21650295-or-it-next-big-thing?utm_content=buffer98228&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Article focused on fairness and serving the unbanked opportunity:

http://betterthancash.org/an-infrastructure-approach-to-improving-financial-inclusion/

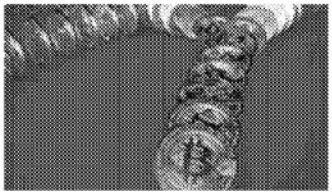
Requires registration, so including all of text of this useful article – which looks through lens of banks at the common ledger strategy:

http://www.thebanker.com/Banking/Blockchain-manoeuvres-applying-Bitcoin-s-technology-to-banking

Blockchain manoeuvres: applying Bitcoin's technology to banking

By Dan Barnes | Published: 14 May, 2015 | Comment on this article

- Print
- Share on emailEmail
- Share
- Recommend
- Comment



Bitcoin's blockchain is being hailed as revolutionary. But will the likes of UBS, ING and Nasdaq, who are exploring the potential of the technology, be able to overcome the challenges that remain, not least security and regulatory issues?

Bitcoin may never fly as a currency but the blockchain – the technology behind Bitcoin – has revolutionary potential. It could transform almost every aspect of commerce and make standard internet transactions seem old fashioned.

Already there are ideas for using the blockchain to make payments faster and cheaper, to make it easier for small businesses to obtain finance and for banks to assess mortgage portfolios at the click of a mouse. Smart trade finance contracts are being worked on that are so watertight, they will never be argued over in court. Securities transactions could be settled in minutes rather than days. Audits and compliance could be done with a fraction of the resources previously used. Many aspects of business, such as wage payment, could be done instantly.

Nasdaq announced in May plans to use a blockchain system for stock issuance on its private market, citing the system's integrity, auditability, governance and transfer of ownership capabilities.

If only half these ideas come to fruition, Bitcoin's blockchain would be a catalyst for technologies that would make web 2.0 or 3.0 seem like something from the Stone Age. "[Smart contracts] are the foundation for a new generation of applications on the internet," says one tech innovator.

Best brains

Obviously there are huge challenges, security and regulatory issues among them. But many banks are putting their best brains to work on research to come up with solutions. UBS, for example, has a team based at Level 39, the tech start-up incubator in London, looking at multiple-use cases and determining how resilient blockchain constructions are. The bank is in good company – the Bank of England reportedly also has people at Level 39 working on blockchain.

"Blockchain could have the potential to change the way we do business in various asset classes. It could have the potential to change identity management in personal and institutional banking," says Oliver Bussmann, group chief information officer at UBS.

Mark Buitenhek, global head of transaction services at ING, says: "The usage is much broader than just a currency. We are focusing on everything else around it. We are taking this extremely seriously. When you talk about disruption in the banking industry, starting with payments, this is one of the most far-reaching technologies that is around."

Model for the future

Ironically for a technology with such revolutionary potential, the Bitcoin/blockchain operating principle is best explained in terms of ancient forms of exchange. For 500 years or more, stone coins called rai, up to 3.6 metres in diameter, have been used on the Pacific island of Yap. The apparent impracticality of the currency is misleading. Ownership of a coin does not require a physical transfer of the rai stone; the owner passes ownership to a new person by word of mouth, along with the historical record of ownership. Transactions are public, as is ownership. The location of the coin, whether at the top of a mountain or the bottom of the sea, is immaterial. However, reciting the correct record of ownership will soon reveal whether the current owner is in legitimate ownership of the coin.

Bitcoin operates in just the same way. Transfer from one account to another involves no coin, simply a continuous record of transactions. This record is encoded in a block, in such a way that it can never be interfered with. The technology that underpins this model of transaction is called the blockchain, an immutable, distributed ledger system that records the transfer between accounts.

A blockchain model consists of three things: the database or ledger; the meaning given to the number of units, for example, one Bitcoin; and the transaction function that confirms a viable transfer from – in the case of Bitcoin – address A to address B.

Using Bitcoin requires the download of software to connect to the network. Likewise, if users want to mine Bitcoins – effectively process settlements – then they need to download Bitcoin mining software. This results in payment by Bitcoin and an encrypted record added to the block, which forms the ledger. Key to the success of technologies based on the blockchain is the information record the ledger creates – using this supply of information has the potential to make arduous processes much simpler.

Security issues

But is it safe? High profile thefts of Bitcoins have caused concerns about its security, but these are not related to the ledger model any more than a theft from an online bank account is related to a centralised ledger system, says Francesco Burelli, partner in the payments practice at strategic management advisory firm InnoValue.

"Similar types of breaches happen to custodians within centralised and distributed ledger ecosystems," he says. "While the distributed ledger is very robust and cannot be tampered with, the anonymity of its transactions and the practical lack of [know your customer verification] and compliance [in Bitcoin], make it more vulnerable at custodian level."

It is the nature of Bitcoin's anonymity, the ability of users to mask IP addresses and the ability to keep the stolen Bitcoin values in peer-to-peer transactions within the Bitcoin ecosystem for an indefinite number of transactions that makes it more vulnerable than institutional payment systems. "That makes investigations and the prosecution of criminals within the Bitcoin ecosystem way more complex than in the incumbent financial services industry," says Mr Burelli.

These challenges are not deterring tech firms and banks from exploring blockchain's possibilities. A number of firms are developing technologies that use the same mathematical cryptographic model as blockchain to work outside of Bitcoin, using custom networks to exchange everything from currency to property contracts, or in some cases even contracts that instruct further actions. The range of possible applications is enormous.

No limits

As blockchain is open source, there are no limits as to who can develop it. More than 100 firms are looking at creating blockchain models for practical business purposes. For Mr Bussmann of UBS, the next stage is the collective adoption of particular systems that are trusted enough to be used by several financial institutions.

"The potential is great, the idea of a distributed ledger that removes complexity is good; the question is how will that work from a workflow perspective, from a scalability perspective and, most importantly, can I trust the involved parties?" he says. "If the industry agrees on a certain standard, then we will see scale and volume exploding. If parties agree this is the most safe, reliable model and regulators are comfortable with it, then volume will come through."

Key to the start-ups is the concept of the contract that is exchanged. Bitcoin is really a tamperproof contract of exchange and the development of increasingly complex contracts offers a wealth of functionality to a blockchain.

Smart contracts

Fintech start-up Diacle is positioning itself to develop the first smart contract so that lawyers are able to make it more binding and link it directly with payment, which would provide a more useful service than a page of a document that could be argued over in a courtroom, which is itself an expensive process.

"With that in mind, the role of a lawyer in a commercial environment is relatively inadequate irrespective of their drafting of an agreement," says Adam Vaziri, director of Diacle. "What we are doing is using blockchain technology, software that both parties to the transaction can run. So when the person delivers the goods, the digital currency is automatically sent to the seller, so what you are creating now is an escrow service without the trust of a third party and the lawyer that is involved in not only providing you with a bit of paper but providing you with enforceability in software."

Another tech start-up Factom offers a permanent, time-stamped record of data in the blockchain to reduce the cost and complexity of conducting audits, managing records and complying with government regulations.

Paul Snow, CEO and lead developer at Factom, says: "Such technology can vastly reduce the amount of reporting that has to be done and this is the real cost savings that could occur. If you can use mathematics to replace regulation, you can vastly decrease the cost of financial transactions and greatly increase their efficiency and speed."

Factom notes that buying mortgage businesses without being able to accurately analyse the acquired contracts has cost banks billions of dollars in fines, which could potentially have been saved if those mortgage records were easily auditable via a ledger model.

Next-generation apps

The breadth of the systems being developed is considerable. At the very open end, Ethereum is developing a system that will allow complex contracts to be exchanged that, depending upon the interaction between them, can trigger further actions via other contracts with the model secured via a distributed ledger model.

Mihai Alisie, one of Ethereum's founders, says: "We have a blockchain that is featureless in a sense and it has embedded within it a programming language that allows people to create all sorts of things that run on top of the blockchain architecture. The building block for Ethereum is a smart contract; it is like a virtual machine or autonomous programme that is maintained by everyone in the network. Inside the contract you can specify what its purpose is. The contracts are the foundations for a new generation of applications on the internet."

Mr Alisie sees the potential for such a system to create a decentralised, autonomous organisation, with actions such as wage payment simply requiring validation in the network.

At the narrower end, Ripple is specifically targeting payments within financial services firms. Chief executive Chris Larsen says: "The protocol really exists at the bottom of that existing payment stack. We are trying to provide a connecting tissue to all of these essentially closed-value exchange systems."

The level of adoption for these platforms has been low so far, however, there are live cases. Germany's Fidor Bank is already using Ripple to underpin one of its payments platforms. Fidor, which has developed its own operating system to facilitate the development of services for customers, is keen to exploit new technologies to create customer choice.

Fidor chief executive Matthias Kröner says: "Each partner has advantages and disadvantages and we want to come up with a payment configurator so the customer can send $50 from the US to the Philippines and preselect a super traditional payment with low risk but paying approximately $10 in commission and taking five days or a newer route that takes five seconds."

Jerry Norton, managing director of financial services at technology provider CGI says that his firm has built a proof of concept within a bank environment between an account and a mobile wallet. "We built an adapter for the bank that talks [universal financial industry standard] ISO20022 one way and talks into the Ripple network at the other. It works, it is running transactions and we have some ideas about how to make it industrial strength."

Many other banks, including ING, are in talks with Ripple to explore the potential of the system as an alternative to the complex and costly model for setting up a payments platform.

ING's Mr Buitenhek says: "Can we use this to replace existing technology, whether for transfers or payments or in the security space? Banks are making the choice to move to a 24/7 real-time payment service: instant payments but also instant business. Discussions of what kind of technology to use is an interesting dilemma: do you go for the brand new, not completely tested but very promising blockchain type of technology with everything in it or proven technology with databases? As the outages have shown in the UK and other countries, people don't accept downtime."

Money has memory

Nasdaq is using a blockchain-based system to enhance its ability to keep track of clients' private issuance of stock. Chief executive Robert Greifeld says: "Our initial application of Nasdaq's blockchain technology-enabled offering will modernise, streamline and secure typically cumbersome administrative functions, and will simplify the overwhelming challenges private companies face with manual ledger record-keeping."

Future applications have exciting potential, including the ability to challenge the concept that 'money has no memory', says Mr Kröner. "We have thought about the memory of money via a blockchain. That's an idea we would love to drill down into, but a little bit further down the road."

UBS's Mr Bussmann says that because any contract could be transacted, if the systems are built securely and adopted widely, the impact is difficult to fathom right now because it could be so deep. "The contract that you manage in blockchain could be a current account. That could disrupt the fundamentals of banking. I simply don't have visibility across five or 10 years to see how far this could go."

Banks could transfer the Bitcoin transaction model to everything from cash micropayments to complex derivatives trades, revolutionising the infrastructure that underpins markets today.

Blockchain settles and records Bitcoin transactions permanently, without any central settlement platform. The Bitcoin element could in principle be replaced by any contract – a virtual bank note, a mortgage or a credit default swap. The principle of having a settlement system inherent within a transaction network would take out an operational layer – the hub that sits between counterparties. The question is whether it could be done in a manner that does not weaken, or even strengthens, that network.

Seeing the potential

Of those banks that recognise blockchain's potential, most are in the early stage of exploring the technology. BNY Mellon decided to start with an internal project that would allow its staff to become familiar with the way the systems work.

Suresh Kumar, chief information officer at BNY Mellon, says: "[Internally] we decided to create a currency called BKoins – named after our stock symbol – with the ability for people to be rewarded in BKoins when there is a collaboration of some sort. We are building this platform and it allows us to download the code, look at the services, put it in our [application programming interface] store and look at developing [user interfaces] for a wallet."

After this the bank plans to work with vendors on building applications, examining their use cases and deciding whether to deploy them. "We are in the exploration and education phase," says Mr Kumar.

However, it is not hard to see where the characteristics of the model could make a practical difference to existing platforms and processes. Mr Bussmann says: "In payments and FX [foreign exchange], one could use a distributed ledger to execute FX trades as a smart contract; cheaper payments for corporate and cross-border for correspondent banking; smart bond issuance and trading; swap settlement on blockchain; loan settlement; loyalty programmes."

Efficiency gains

The potential benefits are also clear. With transaction duplication rendered impossible, a faster settlement cycle, a permanent history of transactions and a considerably simpler apparatus, some great efficiency gains are possible. Post-trade processing is a particular target.

"Currently there are so many different ways for an institution to reconcile transactions, there can be a lack of direct transparency," says Mr Kumar. "It usually works sequentially, which is slow, so from a client experience and service level perspective, it is not optimal. There are benefits, however. Being slow, if someone were to make a mistake, it is easy to correct and there are established practices for correction. Blockchain needs to have similar recourse and legal backing for transactions of large values."

Mr Bussmann adds: "Post-trade reconciliation across a stock exchange and various banks takes T+2 days; if you look at the scenario we are running at the moment, we could see a reduction from days to minutes. All parties are keen to reduce counterparty risk. Plus, if you have settled in minutes you have your securities available to be sold on again."

Chris Dunne, payment services director at Vocalink, the operator of the UK's national payments infrastructure, says that blockchain's simplicity – and therefore transparency – also gives it the potential to tackle some serious issues that dog payments systems today.

"One of the biggest issues with payments is identity; the potential for blockchain to validate who you are to a third party with a high degree of confidence without giving away lots of personal details is interesting," he says. "The other interesting piece is the history of transactions. For the largest banks you can now download your transactions, upload them to a price comparison website, then look back through transactions and identify which bank can give you the best deal."

He says that a logical extension to that model would be for a business to use blockchain as a complete record of incomings and outgoings when interacting with financial services providers. "Small businesses have a lack of ability to shop around for loans and financial products. If you hav e that [record], firms can lend with much higher confidence."

What this will mean for transaction infrastructures is revolutionary. They typically operate the complex post-trade mechanisms that validate and reconcile transactions that senior bankers believe may no longer be necessary.

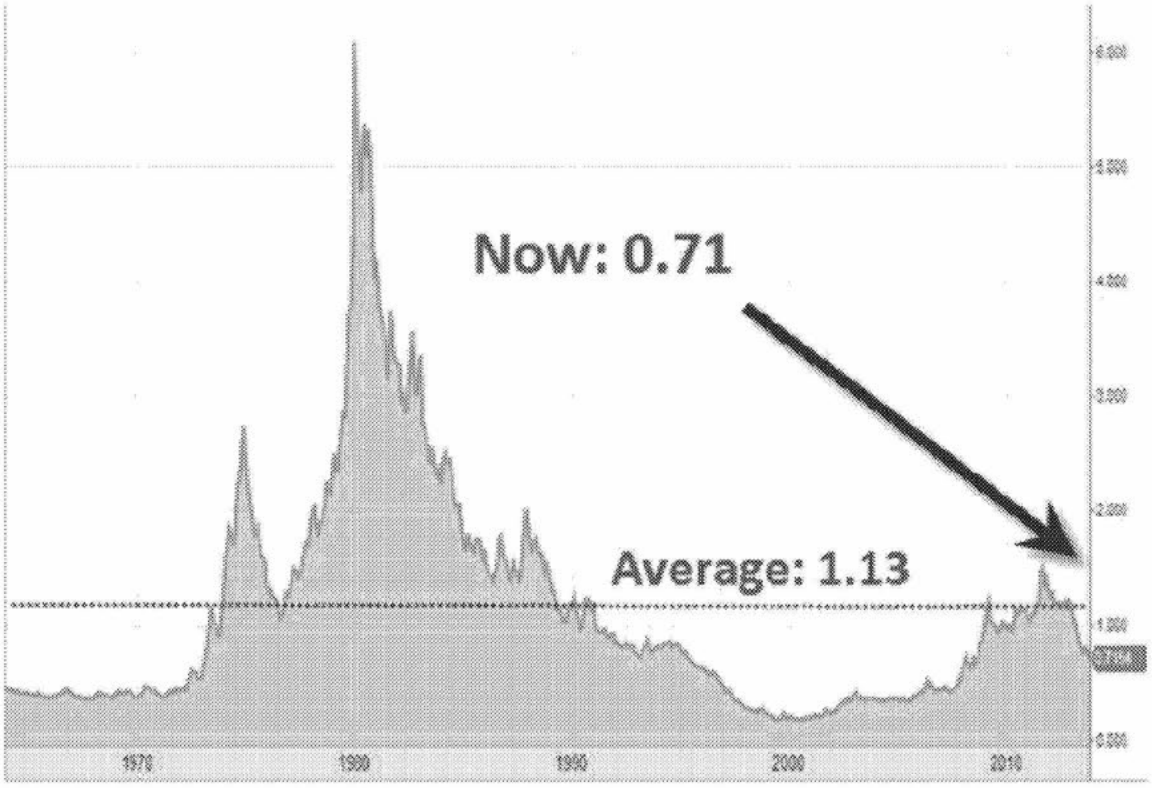
"There could be changes to the [current payments] model of Swift in the future. It could [instead] be part of that ecosystem and could secure the interaction with the general ledger," says Mr Bussmann. "There is significant infrastructure today that reconciles trades across asset classes. I think the time to execution and the way trades are executed will change."

In other words almost anything is possible. In the blockchain age, people will look back on standard internet finance as just a bridge on the way from the analogue world to where the revolution really began.

Other: Gold divided by S&P

Longer chart:

Gold price vs S&P500 since 1964



Source: Opendatadepot, World Bank, St Louis Fed

[redacted]